

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF RHODE ISLAND**

UNITED STATES OF AMERICA)
)
)
VS) CR. NO. 16 – 011 M
)
JASON D. BOUDREAU)

MOTION TO SUPPRESS

Now comes Jason D. Boudreau, the accused in the above captioned matter, and moves to suppress all evidence seized, observations made, and information obtained as a result of the unlawful and warrantless cellphone GPS tracking/“ping” and all evidence seized, observations made and information obtained as a result of a warrantless search done of Mr. Boudreau’s cell phone done at the time of the arrest on December 29, 2015. As reasons, the arrest in Branford, CT on December 29, 2015 only occurred because the agents unlawfully tracked Mr. Boudreau’s cell phone and violated his constitutional rights. Further, all evidence obtained from the warrantless search of the cell phone, including any and all text messages, photographs, and any other digital/electronic evidence was seized illegally and violated his constitutional rights.

Respectfully submitted
JASON D. BOUDREAU
By his attorney,
/s/ Olin Thompson, #5684
Federal Defender
10 Weybosset St., Ste. 300
Providence, RI 02903
(401) 528-4281
Olin.Thompson@fd.org

CERTIFICATION

I hereby certify that a copy of this motion as delivered by electronic notification to AUSAs Denise Barton and Sandra Hebert on May 1, 2017.

/s/ Olin Thompson

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF RHODE ISLAND**

UNITED STATES OF AMERICA)
)
)
VS) CR. NO. 16 – 011 M
)
JASON D. BOUDREAU)

MEMORANDUM IN SUPPORT OF MR. BOUDREAU'S MOTION TO SUPPRESS

Now comes Jason D. Boudreau, the accused in the above captioned matter, and moves to suppress all evidence seized, observations made, and information obtained as a result of the unlawful and warrantless cellphone GPS tracking/“ping” and all evidence seized, observations made and information obtained as a result of a warrantless search of Mr. Boudreau’s cell phone at the time of the arrest on December 29, 2015.

FACTS

On December 29, 2015 Rhode Island State Police (“RISP”) Detective Brian Macera (“Detective Macera”) faxed a “Stored Communication, GPS/Ping Emergency Request Form” to Sprint Corporate Security requesting an emergency cell phone ping for a phone number attributed to Mr. Boudreau. Later that same day, Sprint provided the information requested to Detective Macera. The information showed that between 15:49:18 and 22:05:53 on December 29, 2015, Mr. Boudreau’s cell phone stayed approximately at latitude of 41.28 and longitude of -72.83.

I. Cell Phone Ping/GPS Tracking

A cellular phone is in constant communication with cell towers operated by their phone service. Cal Cumpstone, GAME OF PHONES: THE FOURTH AMENDMENT IMPLICATIONS OF REAL-TIME CELL PHONE TRACKING, 65 Clev. St. L. Rev. 77, (citation omitted). As a cell phone moves it continuously connects with the nearest cell phone tower and reports its location to the phone company. *Id.* (citation omitted). The information conveyed consistently to cell towers is cell site location information (“CLSI”). *Id.* (citation omitted). CLSI is imperative to cell phone tracking and law enforcement agencies rely on it because CLSI can calculate a cell phone’s location within several blocks or even several feet. *Id.* (citation omitted).

Law enforcement agencies can gather CLSI retroactively or in real-time. The police tracked Mr. Boudreau using real-time tracking. Real-time tracking tracks cell phones by “pinging” the target cell phone. *Id.* (citation omitted). Pinging is the electronic signaling to a cell phone, triggering a responsive identification transmission from the target phone. *Id.* (citation omitted). Pinging a cell phone will generate a report providing the target cell phone’s GPS coordinates (as in Mr. Boudreau’s case) or the phone’s nearest cell phone tower, which provides a transmission containing the cell phone’s location. *Id.* (citation omitted). Real-time tracking is undetectable to the phone’s owner. *Id.* (citation omitted).

II. Mr. Boudreau’s Arrest

On December 29th, Homeland Security Ice (“HSI”) and Providence Special Agents traveled to Branford, CT where they located and arrested Mr. Boudreau using the GPS location provided by Sprint. Once in Connecticut, HSI Agents and Providence Detectives met HSI New Haven and the local Branford Police and then located Mr. Boudreau’s rental vehicle outside of a Kohl’s Department Store. Agents proceeded to look around in different establishments until they located

Mr. Boudreau in the Branford Cue & Brew restaurant and bar. HSI Agents Dave Riccio and Brendan Cullen immediately recognized Mr. Boudreau. The manager of the Branford Cue & Brew then supplied the agents with Mr. Boudreau's identification, confirming his identity. Mr. Boudreau was then handcuffed and instructed to lean against a pool table.

While at the Branford Cue & Brew, Agents searched through Mr. Boudreau's phone and took photos of his text messages. As instructed, Mr. Boudreau remained standing by the pool table and handcuffed, when a Branford police K-9 unit entered the bar and the dog bit Mr. Boudreau on his leg above his knee. Understandably concerned for his safety with the Branford Police Department, Mr. Boudreau declined their offer of medical treatment and instead went with the United States Marshalls. He was taken to Wyatt Detention Facility.

LEGAL PRINCIPLES

The United States Constitution guarantees the people the right to be "secure in their persons, houses, papers, and effects, against unreasonable searches and seizures..." *U.S. Const. amend. IV.* Searches and seizures that occur without a warrant are *per se* unreasonable under the Fourth Amendment, with limited exceptions. *See Katz v. United States*, 389 U.S. 347, 357 (1967). In order to determine if there has been a Fourth Amendment violation, courts have looked at whether the government violated an individual's "reasonable expectation of privacy." *See State v. Earls*, 214 N.J. 564, 579 (2013)(citations omitted).

Further, the Fourth Amendment protects people, not places. *See Katz v. United States*, 389 U.S. 347, 351 (1967). In Justice Harlan's concurrence in *Katz*, he put forth a two part test for determining whether an intrusion is unreasonable. "First,... a person [must] have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared

to recognize as ‘reasonable’” *Id.* at 361 (Harlan, J., concurring). This test has subsequently been adopted by the Supreme Court. *See United States v. Jones*, 132 S. Ct. 945, 950 (2012).

ARGUMENT

- I. **Evidence found as a result of Mr. Boudreau’s arrest on December 29, 2015 must be suppressed because the warrantless cell phone “ping” request was illegal and a violation of his Fourth Amendment rights and there was no valid emergency to justify a warrantless cell phone search.**

- a. The cell phone “ping” is a search and requires a warrant

Various state courts have already ruled on this issue and found that cell phone pings are a search and require a warrant. In *State v. Earls*, the New Jersey Supreme Court found that Article I, Paragraph 7 of the New Jersey Constitution – language parallel to that of the Fourth Amendment – protects “an individual’s privacy interest in the location of his or her cell phone” because cell phone users expect confidentiality in the “ever increasing level of detail that cell phones reveal about their lives.” *See Earls*, 214 N.J. at 588. Therefore, police must obtain a warrant based on a showing of probable cause to obtain tracking information through the use of a cell phone.” *Id.* (this case held that the New Jersey equivalent of the Fourth Amendment, Article I, Paragraph 7 of the New Jersey Constitution, required police to obtain a warrant. The language of the New Jersey equivalent is nearly identical to that of the Fourth Amendment and the New Jersey Supreme Court’s ruling relied on and discussed federal case law to make its ruling).

Like New Jersey, the Florida Supreme Court ruled in *Tracey v. State* the defendant had a subjective expectation of privacy in the “location signals transmitted solely to enable the private and personal use of his cell phone, *even on public roads*, and that he did not voluntarily convey that information to the service provider for any other purpose other than to enable use of his cell phone for its intended purpose.” *See Tracey v. State*, 152 S. 3d 504, 525 (Fla. 2014)(emphasis added). Further, the Florida Supreme Court ruled that society is now prepared to recognize the privacy of one’s

location as signaled by one's cell phone as objectively reasonable under the second prong of *Katz*. *Id.* at 526. The Florida Supreme Court analyzed federal precedent (including *United States v. Knotts*, *United States v. Karo*, and *United States v. Skinner*, all cases to be discussed below) and focused on issues including: tracking information being relayed whether or not defendants are in a public or private area and how that can only be determined post hoc, whether someone knowing their cell phone gives off tracking signals does not consents to give their location to law enforcement (the court determined no), and whether cell phones are “effects” under in the Fourth Amendment (court determined they were). *See generally, Id.*

The federal courts, however, are more split on whether electronic tracking, and more specifically cell phone pinging, is considered a search under the Fourth Amendment. *See United States v. Jones*, 132 S. Ct. 945 (2012); *United States v. Karo*, 468 U.S. 705 (1984); *United States v. Knotts*, 460 U.S. 276 (1983); *United States v. Skinner*, 690 F.3d 772 (6th Cir. 2012). In *Knotts*, the Supreme Court upheld the warrantless monitoring of a beeper that law enforcement had placed in a container of chloroform and used to follow the defendant on public streets and highways. *See Knotts*, 460 U.S. at 285. The court reasoned that because the defendant had no reasonable expectation of privacy in his car’s movement on public roads, no warrant was required. *Id.* at 281-82. In *Karo*, however, the Supreme Court found the warrantless monitoring of a beeper, placed in a container of ether, on public roads and in private homes violated the Fourth Amendment. *See Karo*, 468 U.S. at 714.

Only one federal court has addressed the full issue of real-time cell phone tracking. In *United States v. Skinner* the Sixth Circuit, relying on the holding in *Knotts* (a decision predating the popularity and general use of cell phones), held that the defendant had no reasonable expectation of privacy in his movements and any cell phone information regarding his location because he was traveling in an automobile on a public road and that same information could have been gathered by visual surveillance of the defendant driving. Cumpstone, GAME OF PHONES. In *Skinner* the Court analyzed

a fact pattern where Drug Enforcement Agency (DEA) agents believed the defendant to be a drug courier. *Id.* The DEA agents identified the phone number(s) the defendant used and obtained an order from a federal magistrate judge authorizing the phone company to provide subscriber information and location information including real-time cell information and GPS location. *Id.* The police tracked his phone for three days and then arrested him. *Id.*

Skinner is different from Mr. Boudreau's situation, however, in various ways. The key difference between the two is the officers in *Skinner* obtained a court order from a magistrate judge allowing them to track the cell phone. *Id.* The officers in *Skinner* lawfully got a court order for the cell phone information, unlike the officers did in Mr. Boudreau's case, and thus the Court in *Skinner* did not have to consider whether or not a warrantless cell phone ping search was per se unreasonable.

The rationale of the court in *Skinner* is likewise distinguishable from Mr. Boudreau's case and should be read narrowly. The court, in *Skinner*, utilized a limiting rationale when it stated "[i]f a tool used to transport *contraband* gives of [sic] a signal that can be tracked for location, certainly the police can *track* the signal." Cumpstone, GAME OF PHONES (emphasis added). First, In Mr. Boudreau's case, officers ping'ed Mr. Boudreau's cell phone intending to arrest Mr. Boudreau pursuant to an active warrant, they were not investigating him for transporting contraband as the case was in *Skinner*. Second, the court's rationale limits law enforcement to tracking cell phones merely passively and is not applicable to actual active pinging where the officers are intervening to gather information. *Id.* In Mr. Boudreau's case, the officers had Sprint actively ping Mr. Boudreau's cell phone.

The defendant in *Skinner* was travelling on a public highway and the court discussed that fact within its decision. Here, Mr. Boudreau was not traveling on public highways, evidenced by the fact that the pings of his cell phone were in the same general longitude and latitude points over a period

of hours. While Mr. Boudreau ended up not being in a private residence, there was absolutely no way for the police to know that. The only thing the police clearly knew was that Mr. Boudreau was stationary. Unlike in *Skinner*, where the court focused on law enforcement's ability to visually have seen and followed the defendant, in Mr. Boudreau's case the police could not have followed him because he was not moving nor could the police observed Mr. Boudreau through visual surveillance because did not know where he was (hence why they felt compelled to unconstitutionally ping his cell phone).

Other courts have considered portions of the argument analyzed in *Skinner*. For example, in *United States v. Carabollo*, the government argued that the defendant did not have a reasonable expectation of privacy in the cell phone's location the defendant was in a car on a public highway. See *United States v. Carabollo*, 963 F. Supp. 2d 341, 354 (D. Vt. 2013). The Second Circuit, however, had a twofold issue with the government's argument. *Id.* First, the ping data would have been transmitted to law enforcement whether or not the defendant was in his home or on a public highway, and second, there was no means of tracking the defendant's movements using traditional surveillance and the defendant's location was solely obtained through nonpublic technology. *Id.* (citing *United States v. Kyllo*, 533 U.S. 27, 40 (2001) ("Where, as here, the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a 'search' and is presumptively unreasonable without a warrant."))

That is exactly the issue in Mr. Boudreau's case. The ping data led police to find Mr. Boudreau at a bar but the ping would have been given to law enforcement regardless of whether Mr. Boudreau was at the bar or in his home. As mentioned previously, the only thing that the police knew at the time of the cell phone pings was that Mr. Boudreau was not travelling on a public highway but stationary.

Likewise, Mr. Boudreau may have been found in a public place but he was found only after the police used technology not available to the public to locate him. The Supreme Court ruled in *Kyllo* that where the government uses a device not in general public use to obtain information that is unknown without intrusion this constituted a search. *Kyllo*, 533 U.S. 27, 40 (2001). While the facts of *Kyllo* involved using a device to look into the contents of a home, the standard that the public needs to generally use the technology otherwise law enforcement's use of it is unconstitutional should apply in Mr. Boudreau's case. While most people have a cell phone today, the public cannot access cell phone ping information.

Based on the case law, this court should find that a cell phone ping is a search and requires a warrant. The rationale of *Skinner* does not apply to the facts of Mr. Boudreau's case because he was not driving on a public highway, the officers actively (not passively) ping'ed Mr. Boudreau's cell phone, and the officers here did not get a court order.

b. The emergency exception under §2702 did not apply in this case.

18 U.S.C. §2702(c)(4) of the Stored Communications Act authorizes cell phone service providers to disclose without a warrant "a record or other information pertaining to a subscriber to or customer of [cell phone] service... to a governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of information relating to the emergency." *Caraballo*, 963 F. Supp. 2d at 360 (quoting 18 U.S.C. §2702(c)(4)). Congress intended the phrase "other information" to cover location of subscriber's cell phone. *United States v. Gilliam*, 842 F.3d 801, 803 (2nd Cir. 2016)(citing S. Rep. No. 99-541, at 38 (1986)), and the second circuit agreed. Therefore, cell phone pings are subject to the emergency exception of 18 U.S.C. §2702(c)(4).

The issue in Mr. Boudreau's case is whether there was actually an emergency. The test to determine exigent circumstances is an objective one based on the totality of the circumstances. *Caraballo*, 963 F. Supp. 2d at 363 (quoting *United States v. MacDonald*, 916 F.2d 766, 769 (2d Cir. 1990)). Here, there is absolutely no reliable evidence that the police officers actually believed that Mr. Boudreau was planning on killing himself within the time that it would have taken to get a warrant from a judge. The only document mentioning any emergency is Sprint's Emergency Request Form signed by Detective Macera indicating that Mr. Boudreau told his ex-wife he was going to kill himself. There is no information provided in discovery that there was in fact a conversation between Detective Macera and Mr. Boudreau's ex-wife (who is never named anywhere in the discovery) and even if there was the alleged conversation, there is absolutely no evidence that supports the reliability of her alleged statement and that it was in fact an emergency situation. Further, there is no information regarding when she allegedly told the police this information, which law enforcement entity she told, how she told them, or any other circumstances around the alleged statement. Looking at the totality of the circumstances, or the lack thereof in this case, it is not reasonable to believe that an officer would have thought that within the time it would have taken to get a warrant Mr. Boudreau would have actually killed himself. Based on the lack of evidence, there is no showing that there was an exigent circumstance and the emergency exception under 18 U.S.C. §2702(c)(4) does not apply. The arrest and all subsequent evidence should be suppressed.

II. Alternatively, even if the court finds that the “ping” request was legal, the evidence found from the warrantless search of Mr. Boudreau’s cell phone, including but not limited to text messages and internet history, must be suppressed because the warrantless search of Mr. Boudreau’s cell phone was a violation of his Fourth Amendment rights.

Assuming arguendo the court believes the cell phone ping search was constitutional, the court should still suppress the evidence found in the cell phone. The evidence was seized pursuant to a warrantless search in violation of his Fourth Amendment rights.

A warrantless search is per se unreasonable under the Fourth Amendment unless one of the few specifically established exceptions applies. *See Arizona v. Gant*, 556 U.S. 332, 338 (2009)(quoting *Katz v. United States*, 389 U.S. 347, 357 (1967)). One of these specific exceptions is the search-incident-to-arrest doctrine. *See generally Chimel v. California*, 395 U.S. 752 (1969). In *Chimel*, the Court found that the search-incident-to-arrest doctrine permits an arresting officer to “search for and seize any evidence on the arrestee’s person in *order to prevent its concealment or destruction*” and to search the area where an arrestee could reach in “*order to grab a weapon or evidentiary items.*” *Id.* at 763 (emphasis added). The rationale was to prevent the destruction of evidence and protect officer’s safety. *Id.*

The United States Supreme Court has found that absent exigent circumstances, a warrant is required to search someone’s cell phone, even when a cell phone is seized incident to arrest. *See Riley v. California*, 134 S. Ct. 2473, 2493 (2014). The Supreme Court, looking at the rationale for the search-incident-to-arrest outlined in *Chimel v. California* (*Id.* at 2483 (citing *Chimel v. California*, 395 U.S. 752 (1969))) decided neither protecting officer’s safety nor preventing the destruction of evidence support searching cell phone incident to arrest. *Id.* First, the Supreme Court found that “[d]igital data on a stored cell phone cannot itself be used as a weapon to harm an arresting officer...” *Id.* at 2485. Second, the Supreme Court found that the destruction of evidence was not a justifiable reason to search a cell phone either. *See Id. generally* at 2486-2488. The government, in *Riley*, tried to rebut the court’s decision arguing that unless the police searched the phone right away they

risked remote wiping or encryption of the cell phone. *Id.* The Court disagreed with that viewpoint, however, and decided once an officer has the cell phone there is no longer a risk that the arrestee will be able to delete the data himself, an officer can prevent remote wiping in various ways and thus government cannot rely on that argument, and opportunity to look at non-encrypted information is so limited due to password-protection that the argument is moot. *Id.*

The Supreme Court justified their blanket ruling further by elaborating that if the police were “truly confronted” by a “now or never” situation, the police could still rely on the exigent circumstances exception to search the phone (not the search incident to arrest exception). *Id.* at 2487 (citing *Missouri v. McNeely*, 569 U.S. ____ (2013)(citations omitted)). The exigent circumstances doctrine applies when “the exigencies of the situation’ make the needs of law enforcement *so compelling* that [a] warrantless search is objectively reasonable under the Fourth Amendment.” *Id.* at 2494 (citing *Kentucky v. King*, 563 U.S. at 460)(citation omitted))(emphasis added). The court provided examples of exigent circumstances including, a suspect texting an accomplice who is going to detonate a bomb, or a child abductor who may have information regarding the child on his phone. *Id.* at 2494.

In Mr. Boudreau’s case the blanket rule against warrantless cell phone searches incident to arrest applies. As the Supreme Court states, law enforcement had no reason to fear their own safety or be concerned about the destruction of evidence. *See generally Riley. California*, 143 S. Ct. 2473. Likewise, there was no “exigent circumstance” that would have given the government a compelling interest allowing law enforcement to search Mr. Boudreau’s phone right then. The actions of the police on December 29, 2015 are objectively unreasonable under the Fourth Amendment, they violated Mr. Boudreau’s constitutional rights, and thus the evidence found from the cell phone and subsequently based on that search must be suppressed.

CONCLUSION

Wherefore, because the cell phone ping was a search, there is no evidence of an emergency justifying the warrantless search, and the search of Mr. Boudreau's cell phone was unlawful, Mr. Boudreau moves this Honorable Court to suppress any and all evidence found pursuant to Mr. Boudreau's arrest on December 29, 2015.

Respectfully submitted
JASON D. BOUDREAU
By his attorney,
/s/ Olin Thompson, #5684
Federal Defender
10 Weybosset St., Ste. 300
Providence, RI 02903
(401) 528-4281
Olin.Thompson@fd.org

CERTIFICATION

I hereby certify that a copy of this motion as delivered by electronic notification to AUSAs Denise Barton and Sandra Hebert on May 1, 2017.

/s/ Olin Thompson